REMARKS

Claims 1, 14-20, 22-32, and 34 are pending in this application.

Applicants have amended claims 27, 28, and 30. The changes to these claims made herein do not introduce any new matter.

Claim Objections

In Paragraph 7 of the Office Action (see page 3), the Examiner raised an objection to claims 30 and 31, alleging that the phrase "a computer readable storage medium" lacks proper antecedent basis. Applicants do not understand the basis for this objection. In claim 30, the first recitation of the phrase "computer readable storage medium" is preceded by the indefinite article "a." As such, claim 30 does not run afoul of the antecedent basis requirement. Accordingly, reconsideration and removal of the objection to claims 30 and 31 is respectfully requested.

In Paragraph 8 of the Office Action (see page 3), the Examiner raised an objection to claims 32 and 34, alleging that the phrase "portable data carrier" lacks proper antecedent basis. Again, Applicants do not understand the basis for this objection. In claim 32, the recitation of the phrase "portable data carrier" is preceded by the indefinite article "a." As such, claim 32 does not run afoul of the antecedent basis requirement. Accordingly, reconsideration and removal of the objection to claims 32 and 34 is respectfully requested.

Rejections Under 35 U.S.C. § 101

Applicants respectfully request reconsideration of the rejection of claims 27-29 under 35 U.S.C. § 101 as being directed toward non-statutory subject matter. Applicants have amended independent claim 27 to specify that each operation of the method for determining the key for the cryptographic calculation is executed by an integrated circuit. As such, the method defined in present claim 27 is tied to a particular machine. Accordingly, present

claims 27-29 define statutory subject matter under 35 U.S.C. § 101, and Applicants request that the rejection of these claims thereunder be withdrawn.

Applicants respectfully request reconsideration of the rejection of claims 30 and 31 under 35 U.S.C. § 101 as being directed toward non-statutory subject matter. In response to the Examiner's concern that the claimed subject matter includes non-statutory subject matter such as, for example, a signal communicated via a computer network, Applicants have amended independent claim 30 to specify that the computer readable storage medium is a physical medium. Accordingly, present claims 30 and 31 define statutory subject matter under 35 U.S.C. § 101, and Applicants request that the rejection of these claims thereunder be withdrawn.

Rejections Under 35 U.S.C. § 103

Applicants respectfully request reconsideration of the rejection of claims 1, 14, 15, 17, 19-22, 25, 27, 30, and 32 under 35 U.S.C. § 103(a) as being unpatentable over *Walmsley et al.* ("*Walmsley*") (US 2003/0159036 A1) in view of *Sabin* (US 6,959,091 B1). As will be explained in more detail below, the combination of *Walmsley* of in view of *Sabin* would not have rendered the subject matter defined in independent claims 1, 27, 30, and 32, as presented herein, obvious to one having ordinary skill in the art.

Independent Claim1

Independent claim 1 recites as follows (with the feature numbers shown in parentheses being added):

> A method for protected execution of a cryptographic calculation, in which
> (1) a key with at least two key parameters is drawn on, wherein
> (1.1) the key is a private key for use in an RSA method, wherein
> (1.2) each key parameter is contained in the private key, wherein
> (2) an integrity check of the key is performed in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter, wherein

(3) the cryptographic calculation is one of a decryption in the RSA method and a signature generation in the RSA method, and wherein

(4) each operation of the method for protected execution of the cryptographic calculation is executed by an integrated circuit.

In support of the obviousness rejection, the Office Action refers to various paragraphs of *Walmsley* as allegedly teaching all of features (1), (1.1), (1.2), (2), and (4); *Sabin* was cited with respect to only feature (3). However, the Office Action cited various different elements of *Walmsley* as allegedly being the key and the key parameters in each of features (1), (1.1), (1.2), and (2). For example, the Examiner cited the private key K_A of Paragraphs [0486]-[0489] of *Walmsley* as the key in features (1), (1.1), and (1.2), but then cited other elements of *Walmsley* – namely the keys K_1 and K_2 and the values R and M – as the key in feature (2). Applicants submit that this is not permissible. What the Examiner would need to do – but has not done – is to identify a single element of *Walmsley* that can be equated with the key in all features of claim 1. What the Examiner would further need to do – but has not done – is to identify a single group of elements of *Walmsley* that can be equated with the key parameters in all features of claim 1.

Turning to features (1), (1.1), and (1.2) of claim 1 in more detail, in support of the obviousness rejection, the Examiner refers to Paragraphs [0486]-[0489] and [0057]-[0066] of the *Walmsley* reference. Paragraphs [0486]-[0489] disclose a protocol in which a private key K_A is used for decryption in an asymmetric cryptographic method. Paragraphs [0057]-[0066] discuss asymmetric cryptography in general. While Paragraphs [0486]-[0489] of *Walmsley* do indeed disclose a private key K_A, there is no disclosure in these paragraphs of any key parameters, let alone of any *key parameters contained in the private key*, as recited in feature (1.2).

With respect to feature (1.1), it is true that *Walmsley* refers to the RSA method in Paragraphs [0075]-[0078] (not cited in the Office Action). However, there is no teaching that

the asymmetric cryptographic method mentioned in Paragraph [0487] is an RSA method, and not another asymmetric cryptographic method such as the DSA and ElGamal methods set forth in Paragraphs [0079]-[0090] of *Walmsley*.

Turning to feature (2), in support of the obviousness rejection, the Examiner refers to Paragraphs [0545], [0601]-[0606], [0628], [0629], [0652], [0657], [0944], and [0954]-[0957] of *Walmsley*. These paragraphs will now be discussed in detail.

Paragraph [0545] of *Walmsley* reads as follows:

> [0545] An attacker cannot call Prove without a valid R|S[R] pair encrypted with K_1. K_2 is therefore resistant to a chosen text attack. R only advances with a valid call to Test, so K_1 also not susceptible to a chosen text attack.

The above paragraph does <u>not</u> refer to the private key K_A that the Examiner identified as the key of present claim 1. Furthermore, the above paragraph does <u>not</u> refer to any key parameters contained in the private key K_A, nor to any key parameters contained in the keys K_1 and K_2. Moreover, the above paragraph does <u>not</u> teach any integrity check of any key, let alone an integrity check that is performed in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter, as recited in feature (2) of claim 1.

Paragraphs [0601]-[0606] describe the steps shown in Figure 6 of *Walmsley*. These paragraphs refer to keys K_1 and K_2, which are <u>different from</u> the private key K_A that the Examiner identified as the key of present claim 1. Furthermore, Paragraphs [0601]-[0606] do <u>not</u> refer to any key parameters contained in the private key K_A, nor to any key parameters contained in the keys K_1 and K_2. Moreover, Paragraphs [0601]-[0606] do <u>not</u> teach any integrity check of any key, let alone an integrity check that is performed in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter, as recited in feature (2) of claim 1.

Paragraphs [0628] and [0629] of *Walmsley* read as follows:

> [0628] R ChipT only. Current random number. Does not have to be secret, but must be seeded with a different initial value for each chip instance. Changes with each successful authentication as defined by the Test function.
>
> [0629] M Memory vector of authentication chip. Part of this space should be different for each chip (does not have to be a random number).

Paragraphs [0628] and [0629] do not refer to any key, let alone to the private key K_A that the Examiner identified as the key of present claim 1. Paragraphs [0628] and [0629] also do not teach any key parameters. Moreover, Paragraphs [0628] and [0629] do not teach any integrity check of any key, let alone an integrity check that is performed in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter, as recited in feature (2) of claim 1.

Paragraphs [0652] and [0657] read as follows:

> [0652] Only a valid ChipA would know the value of R, since R is not passed into the authenticate function (it is passed in as an encrypted value). R must be obtained by decrypting E[R], which can only be done using the secret key K_A. Once obtained, R must be appended to M and then the result re-encoded. ChipT can then verify that the decoded form of $E_{KA}[R|M]=R|M$ and hence ChipA is valid. Since $K_T \neq K_A$, $E_{KT}[R]¼ E_{KA}[R]$.
>
> [0657] Since ChipT and ChipA contain different keys, intense testing of ChipT will reveal nothing about K_A.

Paragraphs [0652] and [0657] describe the steps of protocol C2, while Paragraphs [0486]-[0489] describe the steps of protocol P2. These are clearly *different* protocols. There is no indication in *Walmsley* that the secret key K_A mentioned in Paragraphs [0652] and [0657] might be the same as the private key K_A (Paragraphs [0486]-[0489]) that the Examiner identified as the key of present claim 1. Furthermore, Paragraphs [0652] and [0657] do not teach any key parameters contained in the private key K_A.

Moreover, Paragraphs [0652] and [0657] do not teach any *integrity check of any key*. According to Paragraph [0652], ChipT verifies that the equation $E_{KA}[R|M]=R|M$ holds. However, this verification concerns the values R and M. As stated in Paragraphs [0628] and

[0629], the value R is a current random number, and the value M is a memory vector. Neither of these values is a key. Consequently, even if evaluation of the equation $E_{KA}[R|M]=R|M$ might be considered as a kind of check of some data values, it is not an integrity check of any *key*, let alone of the private key K_A that the Examiner identified as the key of present claim 1.

Yet further, Paragraphs [0652] and [0657] do not teach any integrity check that is performed in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter, as recited in feature (2) of claim 1. When Paragraph [0657] states that "intense testing of ChipT will reveal nothing about K_A," then this is not the result of any integrity check, but simply the consequence that ChipT does not contain the key K_A. Moreover "intense testing" of ChipT is not a cryptographic attack in which at least one first key parameter is corrupted, as specified in feature (2) of claim 1.

Paragraph [0944] reads as follows:

> [0944] The Checksum register is a 160-bit number used to verify that K_1 and K_2 have not been altered by an attacker. Checksum is programmed along with K_1, K_2 and R with the authentication chip's SSI (Set Secret Information) command. Since Checksum must be kept secret, clients cannot directly read Checksum.

The above paragraph does not refer to the private key K_A that the Examiner identified as the key of present claim 1, let alone to any integrity check performed on this key K_A. Furthermore, the above paragraph does not refer to any key parameters contained in the private key K_A, nor to any key parameters contained in the keys K_1 and K_2. Moreover, the above paragraph does not teach any integrity check that is performed in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter, as recited in feature (2) of claim 1.

Paragraphs [0954]-[0957] describe the use of a random number R and an IsTrusted bit. Neither the random number R nor the IsTrusted bit is a key. Paragraphs [0954]-[0957] further refer to key K_1, which clearly is different from the private key K_A that the Examiner

identified as the key of present claim 1. Furthermore, Paragraphs [0954]-[0957] do not refer to any key parameters contained in the private key K_A, nor to any key parameters contained in the key K_1. Moreover, the above paragraphs do not teach any integrity check of any key, let alone an integrity check that is performed in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter, as recited in feature (2) of claim 1.

In view of the foregoing, the *Walmsley* reference does not disclose each and every aspect of features (1), (1.1), (1.2), (2), and (4) of present claim 1. As the *Sabin* reference was cited with respect to only feature (3), even a combination of the *Walmsley* and *Sabin* references would not have resulted in a method that includes each and every feature of present claim 1. As such, the combination of the *Walmsley* and *Sabin* references would not have rendered the subject matter defined in present claim 1 obvious to one having ordinary skill in the art.

Accordingly, independent claim 1, as presented herein, is patentable under 35 U.S.C. § 103(a) over the combination of *Walmsley* in view of *Sabin*.

Independent Claims 27, 30, and 32

Present independent claims 27, 30, and 32 contain the same features (1), (1.1), (1.2), (2), (3), and (4) as specified in present claim 1, with the exception that present claims 30 and 32 do not explicitly include feature (4). Therefore, independent claims 27, 30, and 32, as presented herein, are patentable under 35 U.S.C. § 103(a) over the combination of *Walmsley* in view of *Sabin* for at least the same reasons set forth in the above detailed discussion of present claim 1.

Dependent Claims 14, 15, 19, 20, 22, and 25

Each of claims 14, 15, 19, 20, 22, and 25 depends from independent claim 1. Claims 14, 15, 19, 20, 22, and 25 are therefore patentable under 35 U.S.C. § 103(a) over the combination of *Walmsley* in view of *Sabin* for at least the same reasons set forth above regarding claim 1.

Dependent Claims 16, 17, 18, 23, 24, 26, 28, 29, 31, and 34

Applicants respectfully request reconsideration of the rejection of claims 16-18, 23, 24, 26, 28, 29, 31, and 34 under 35 U.S.C. § 103(a) as being unpatentable over *Walmsley* in view of *Sabin* and further in view of *Ngo et al.* ("*Ngo*") (US 2003/0097628 A1). Each of claims 16-18, 23, 24, and 26 ultimately depends from independent claim 1. Each of claims 28 and 29 depends from independent claim 27. Claim 31 depends from independent claim 30, and claim 34 depends from independent claim 32. The *Ngo* reference does not cure the above-discussed deficiencies of the *Walmsley* and *Sabin* references relative to the subject matter defined in the present independent claims 1, 27, 30, and 32. Claims 16-18, 23, 24, 26, 28, 29, 31, and 34 are therefore patentable under 35 U.S.C. § 103(a) over the combination of *Walmsley* in view of *Sabin* and further in view of *Ngo* for at least the same reasons set forth above regarding the applicable independent claim.

Conclusion

In view of the foregoing, Applicants respectfully request reconsideration and reexamination of claims 1, 14-20, 22-32, and 34, as amended herein, and submit that these claims are in condition for allowance. Accordingly, a notice of allowance is respectfully requested. In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at **(408) 749-6902**. If any additional

fees are due in connection with the filing of this paper, then the Commissioner is authorized to charge such fees to Deposit Account No. 50-0805 (Order No. WACHP006).

Respectfully submitted,
MARTINE PENILLA & GENCARELLA, L.L.P.

/Peter B. Martine/

Peter B. Martine
Reg. No. 32,043

710 Lakeway Drive, Suite 200
Sunnyvale, California 94085
Customer Number 25920